

512-CD-002-002

## **EOSDIS Core System Project**

# **Release B Maintainability Demonstration Test Plans for the ECS Project**

August 1998

Raytheon Systems Company  
Upper Marlboro, Maryland

# **Release B Maintainability Demonstration Test Plans for the ECS Project**

**August 1998**

Prepared Under Contract NAS5-60000  
CDRL Item # 085

## **SUBMITTED BY**

T W Fisher /s/

8/27/98

Terry Fisher, Release B CCB Chairman  
EOSDIS Core System Project

Date

**Raytheon Systems Company**  
Upper Marlboro, Maryland

This page intentionally left blank.

# Preface

---

This document is a formal contract deliverable with an approval code 1. It requires Government review and approval prior to acceptance and use. This document is under ECS contractor configuration control. Once this document is approved, Contractor approved changes are handled in accordance with Class I and Class II change control requirements described in the EOS Configuration Management Plan, and changes to this document shall be made by document change notice (DCN) or by complete revision.

Any questions should be addressed to:

Data Management Office  
The ECS Project Office  
Raytheon Systems Company  
1616 McCormick Drive  
Upper Marlboro, Maryland 20774-5301

This page intentionally left blank.

# Abstract

---

The Maintainability Demonstration (MD) Test Plans (DID 512) restate the requirements and objectives for conducting MD tests of ECS Commercial Off-The-Shelf (COTS) hardware. The test plans attached are based upon accepted DID 511 MD failure scenarios for Release B that meet the defined MD objectives, and utilize planned Acceptance Test (AT) test procedures. The test plans describe testing requirements, methodology and step-by-step procedure, expected results, and success criteria. The Science and MSS Failover procedures are under development as of this submission, and subject to further change and redlines as a result of dry run or formal testing. The FOS Failover test plan was delivered in the previous submission of DID 512, and is being updated and revised.

**Keywords:** Maintainability, mean down time (MDT), failure, COTS, hardware, RMA, repair, fault, diagnostics, spares, maintenance

This page intentionally left blank.

# Change Information Page

List of Effective Pages			
Page Number		Issue	
Title		Original	
I through x		Original	
1-1 through 1-2		Original	
2-1 through 2-2		Original	
3-1 through 3-4		Original	
4-1 through 4-4		Original	
A-1 through A-8		Original	
B-1 through B-2		Original	
C-1 through C-2		Original	
D-1 through D-2		Original	
AB-1 through AB-2		Original	
Document History			
Document Number	Status/Issue	Publication Date	CCR Number
512-CD-002-001	Original	January 1998	97-1768
512-CD-002-002	Original	August 1998	98-0950

This page intentionally left blank.

# Contents

---

## 1. Introduction

1.1	Identification .....	1-1
1.2	Scope .....	1-1
1.3	Purpose .....	1-1
1.4	Status and Schedule .....	1-2
1.5	Organization .....	1-2

## 2. Related Documentation

2.1	Parent Documents .....	2-1
2.2	Applicable Documents .....	2-1

## 3. ECS Maintainability Environment

3.1	COTS Hardware.....	3-1
3.2	ECS Maintenance and Operations .....	3-1
3.3	Operational Availability (Ao) and Mean Down Time (MDT).....	3-2

## 4. Maintainability Demonstration (MD) Process and Objectives

4.1	Process .....	4-1
4.2	MD Objectives.....	4-1
4.2.1	Verify Capability to Meet Ao and MDT .....	4-1
4.2.2	Evaluate Fault Detection/Isolation Methods .....	4-2
4.2.3	Evaluate Ability to Achieve Line Replaceable Unit (LRU) Replacements On-site .....	4-2

## **Tables**

3-1	ECS Operational Requirements.....	3-3
-----	-----------------------------------	-----

### **Appendix A      Failure Scenarios**

### **Appendix B      FOS Failure Recovery and Status Monitoring Test Plan**

### **Appendix C      Science Ingest Failover Test Plan**

### **Appendix D      MSS Critical Services Failover Test Plan**

### **Abbreviations and Acronyms**

# **1. Introduction**

---

## **1.1 Identification**

This document, Contract Data Requirements List (CDRL) item 085, whose requirements are specified in Data Item Description (DID) 512/PA1, is a required deliverable under the Earth Observing System Data and Information System (EOSDIS) Core System (ECS), Contract NAS5-60000.

## **1.2 Scope**

This document is based upon DID 511 and applies to COTS hardware selected, procured, integrated and tested for an operational ECS Release. The MD Plan DID 511 will be revised in the event of developing custom hardware, but ECS is not planning to develop any custom hardware. The MD Plan also does not apply to the maintainability of ECS-developed or COTS software. The ECS COTS hardware has been designed to commercial maintainability standards and support practices. Therefore, these MD test plans do not verify unit level COTS Mean Time to Repair (MTTR) or commercial maintainability design. The previous submission of DID 512 provided a FOS test plan that met the defined FOS MD objectives for Release B, but this test plan will be revised and updated before dry run and formal testing. This submission identifies the test plans currently in the Acceptance Test and System Verification schedule that support the MD scenarios, and the Ingest and MSS Failover test plans under development.

This document reflects the Feb 7, 1996 Technical Baseline maintained by the contractor Configuration Control Board (CCB) in accordance with ECS Technical Direction # 11, dated December 6, 1994.

## **1.3 Purpose**

The MD Test Plans restate the requirements and objectives for conducting MD tests of ECS COTS hardware. The test plans attached are based upon accepted DID 511 MD failure scenarios for Release B, that meet the defined MD objectives, and utilize planned Acceptance Test and System Verification test procedures. The test plans describe testing requirements, methodology and step-by-step procedure, expected results, and success criteria. The Science and MSS Failover test plans are not complete as of this submission, and subject to further change and redlines as a result of dry run or formal testing. The FOS Failure Recovery and Status Monitoring test plan was delivered in the previous submission of DID 512, and is being updated and revised.

## **1.4 Status and Schedule**

DID 511 for Release B was delivered and approved as one Plan including both FOS and Science failure scenarios, and DID 512 will also be delivered as one document. Since schedule timing

differences exist between FOS and Science the FOS test plan was delivered in the previous submission of DID 512 but will be updated as a result of formal testing and redesign. This submission of DID 512 identifies the existing test plans currently in the Release B v2.0 schedule that support the MD Plan scenarios, and identifies the FOS, Science Ingest and MSS Failover test plans under development.

## **1.5 Organization**

The contents of this document are as follows:

- Section 1: Introduction - Introduces the Maintainability Demonstration Plan scope, purpose, schedule, and document organization.
- Section 2: Related Documentation - Describes the parent and applicable documents useful in understanding the details of subjects discussed in this document.
- Section 3: ECS Maintainability Environment - Discusses COTS hardware maintainability characteristics, Release B operations and maintenance planning, and ECS system functional RMA requirements.
- Section 4: MD Process and Objectives - Describes the implementation process for the MD Plan and the 3 MD objectives and how they are achieved.
- Appendix A: Failure Scenarios - Failure Scenarios MD 1-8.
- Appendix B: FOS Failure Recovery and Status Monitoring Test Plan.
- Appendix C: Science Ingest Failover Test Plan.
- Appendix D: MSS Critical Services Failover Test Plan.

## 2. Related Documentation

---

### 2.1 Parent Documents

The parent documents are the documents from which this Maintainability Demonstration Test Plan's scope and content are derived.

420-05-03	Goddard Space Flight Center, Earth Observing System (EOS) Performance Assurance Requirements for the EOSDIS Core System (ECS)
423-41-01	Goddard Space Flight Center, EOSDIS Core System (ECS) Statement of Work
423-41-02	Goddard Space Fight Center, Functional and Performance Requirements Specification for the EOSDIS Core System (ECS)

### 2.2 Applicable Documents

The following documents are referenced within this Maintainability Demonstration Test Plan or are directly applicable, or contain policies or other directive matters that are binding upon the content of this volume:

322/411-CD-007-002	Flight Operations Segment (FOS) Release B Integration and Acceptance Test Procedures for the ECS Project -- Merged Submission  Release B v2.0 Acceptance Test Procedures
511-CD-002-002	Release B Maintainability Demonstration Plan for the ECS Project
517-CD-001-004	Release B Failure Modes and Effects Analysis and Critical Items List for the ECS Project
613-CD-002-001	COTS Maintenance Plan for the ECS Project

This page intentionally left blank.

## 3. ECS Maintainability Environment

---

### 3.1 COTS Hardware

The ECS hardware for Release B and for Release B FOS is COTS, with no custom hardware or modified COTS planned or expected. The COTS hardware has been designed and built to commercial maintainability standards and practices. This characterizes the COTS hardware as:

1. Modular in design and fabrication.
2. Designed to efficiently troubleshoot and maintain.
3. Maintained by isolating failures to and replacing Line Replaceable Units (LRUs).
4. Typical Mean Time To Repair (MTTR) from 1/2 to 1 hour.
5. Some level of vendor diagnostics will assist trouble shooting.
6. No Preventive Maintenance normally required.
7. No special tools or test, measuring, diagnostic equipment normally required.

Most COTS hardware manufacturers offer warranty and extended warranty maintenance support for their products through their own service/support organizations. They are therefore motivated to design in maintainability to minimize their own support time and materiel costs. Their maintenance technicians are generally well trained, certified, and have access to sophisticated diagnostics and back-up help desks.

These COTS maintainability factors support an MD planning approach that assumes the inherent commercial maintainability of ECS COTS hardware, and does not require evaluating the maintainability design or demonstrating the MTTR of any unit level COTS hardware product.

### 3.2 ECS Maintenance and Operations

Once operations commence, COTS maintenance coverage to the DAACs, System Monitoring and Coordination Center (SMC), and EOS Operations Center (EOC) will be consistent with the operations requirements of ECS-supported missions (e.g. AM-1, Landsat 7, etc.). Because of the higher costs of maintenance support during extended operations hours (i.e. nights, weekends, and holidays), maintenance coverage during these periods will be tailored to that required to sustain mission-critical operations and to satisfy ECS Operational Availability (Ao) and Mean Down Time (MDT) requirements. The minimum Principal Period of Maintenance (PPM) at the DAACs, EOC, SMC, and ECS Development Facility (EDF) will be 8AM to 5PM local, Monday through Friday, excluding local holidays.

An on-site maintenance capability is provided by Local Maintenance Coordinators (LMCs) to satisfy the operational availability and MDT requirements for some ECS functions (e.g. communications and science processing). Factors considered in the selection of COTS hardware

(HW) to be maintained by LMCs include: criticality of the equipment and redundancy of components/systems; technical expertise needed to diagnose and replace failed LRUs; and the cost of training, spares, and support equipment.

LMCs may be trained and certified to perform maintenance on selected ECS equipment. Where the LMC has been designated as the principal maintenance provider for COTS HW and software (SW), his responsibilities include fault diagnostics and identification to the LRU level; replacement of specified failed LRUs; or escalating the problem to the responsible COTS contractor or the SMC for further assistance in diagnosing the cause of the problem.

When a COTS problem occurs, the LMC uses diagnostics tools, such as OpenView and built-in diagnostics, to identify and isolate the problem to the malfunctioning component, which may be SW or a failed LRU. If HW is identified as the source, the LMC or COTS maintenance contractor corrects the problem by replacing the failed LRU, putting the unit back into operation, and testing the equipment and subsystem to verify the problem has been corrected.

Site engineering staffs and their LMC may be unable to resolve some of the more difficult maintenance problems. For this reason, backup support is available from a number of sources, including the SMC, Sustaining Engineering Organizations (SEO), maintenance subcontractors, and Original Equipment Manufacturers (OEMs). The LMC, following local procedures and ECS policy, determines if backup support is required based upon the nature of the problem. Network and SW-related problems may be referred to the SMC for assistance, while HW problems are normally referred to the local COTS hardware maintenance subcontractor for resolution.

### **3.3 Operational Availability (Ao) and Mean Down Time (MDT)**

The ECS  $A_O$  and MDT requirements differ between the FOS, Science Data Processing Segment (SDPS), and Communications and Systems Management Segment (CSMS) functions, depending on the criticality of the function involved. The specific  $A_O$  and MDT objectives for the segments and functions within segments are stated in Section 5 of GSFC 423-41-02, Revision A, dated June 2, 1994, and are shown in Table 3-1, "ECS Operational Requirements." It is emphasized that these requirements do not apply to individual/unit level COTS hardware products, but rather apply to the entire system or sub-system function as indicated in the table.

Downtime has the greatest influence on achieving  $A_O$  in the mathematical relationship, and also is emphasized through its own MDT requirements. These are downtime averages (mean) across all COTS hardware failures in the function over a period of time. When averaging multiple failures, those with long downtime delays can be offset by short downtime switchover corrected failures in the computation of MDT. The MDT requirement is not a discrete amount of time allowed for each individual unit level failure, and should not be measured or demonstrated as such.

**Table 3-1. ECS Operational Requirements**

ECS Functions		A <sub>O</sub> Minimum	MDT Maximum
	<b>Flight Operations Segment (FOS)</b>		
3800	Critical Real-time Functions*	0.9998	1 Min.
3810	Non-Critical Real-time Functions*	0.99925	5 Min.
3820	Targets of Opportunity (TOO) *	0.992	1 Hr
3700	ECS Functions not Otherwise Specified	0.96	4 Hrs
3710	ECS shall have no single point of failure for functions associated with real time operations of the spacecraft and instruments		
	<b>Science Data Processing Segment (SDPS)</b>		
3900	Science Data Receiving	0.999	2 Hrs
3910	Switch over from Primary Science Data Receipt to Backup	NA	15 Min. Maximum not MDT
3920	Archiving & Distributing Data	0.98	2 Hrs
3930	User Interfaces to IMS Services at DAACs	0.993	2 Hrs
3940	Information Searches on the ECS Directory	0.993	2 Hrs
3950	Data Acquisition Request Submittals including TOOs*	0.993	2 Hrs
3960	Metadata Ingest and Update	0.96	4 Hrs
3970	Information Searches on Local Holdings	0.96	4 Hrs
3980	Local Data Order Submission	0.96	4 Hrs
3990	Data Order Submission Across DAACs	0.96	4 Hrs
4000	IMS Data Base Management and Maintenance Interface	0.96	4 Hrs
4010	Product Generation Computers	0.95	NA
4020	Product generation computers shall provide a "Fail soft" environment		
	<b>Communications and System Monitoring Segment (CSMS)</b>		
4030	SMC function of gathering and disseminating system management information, for critical services	0.998	20 Min.
4035	ESN shall have no single point of failure for functions associated with network databases and configuration data		
4036	ESN A <sub>O</sub> shall be consistent with the specified A <sub>O</sub> of the ECS functions.		
3630	Maximum down time shall not exceed twice the required MDT in 99 percent of failure occurrences		
A <sub>O</sub> = Operational Availability MDT= Mean Down Time		* = Required for Release B and subsequent releases only (all other functions required for Release A and subsequent releases)	

This page intentionally left blank.

## **4. Maintainability Demonstration (MD) Process and Objectives**

---

### **4.1 Process**

The EOS Performance Assurance Requirements for the ECS, GSFC 420-05-03, in RMA Section 5.6, presents the MD process and objectives. In accordance with this guidance, the approved DID 511 presented proposed failure scenarios to achieve the MD objectives. Test plans are identified in these scenarios in DID 512, that will be conducted as part of the Acceptance Test and System Verification program. The test plans identified are existing AT and Verification test procedures with similar objectives, and two (2) new Failover tests under development. AT test procedures and MD scenarios with the same objectives are coordinated into one testing activity serving both needs, rather than accomplishing redundant tests. Since the existing AT and SV test procedures referenced are available on the World Wide Web, they are not included as attachments to this DID. This coordination is demonstrated by the use of FOS Test Case SYS-2030B in attachment B. This coordination of testing will be described appropriately in the MD Test Report, DID 519.

### **4.2 MD Objectives**

The Performance Assurance Requirements (PAR) Section 5.6 and DID 511 establish three objectives for the Maintainability Demonstrations. These are discussed below and related to the specific MD failure scenarios in Appendix A.

#### **4.2.1 Verify Capability to Meet Ao and MDT**

The objective of the demonstrations as stated in the PAR is to verify the capability of the planned maintenance activities to meet the operational availability/mean down times (Ao/MDT) stated in the ECS F&P Specification for identified system functions. The PAR Section 5.6 identifies the system functions as the critical real-time system functions (primarily in the FOS).

As discussed in Section 3.3, the F&P specification RMA requirements are system function requirements applying across all the COTS hardware implementing that function. An MD test, however, is normally accomplished on one individual unit level COTS product, and any resulting downtime measure for ECS would not represent all the COTS hardware in the function for the given time period. Also, Ao is not directly measurable through an MD test; but the principal component downtime is.

ECS critical real-time system functions are specified and exist only in the FOS. Since the MDT requirements for these are one (1) minute or less, they are only achievable through hardware redundancy in the design and software switchover in the event of failure. This switchover is demonstrable through testing and will achieve this MD objective. Failure scenarios to demonstrate switchover are proposed for the FOS critical real-time functions during Release B.

These are included in Appendix A as scenarios MD - 6 and 8 for Release B. The applicable test plan is FOS Test Case SYS-2030B (Failure Recovery and Status Monitoring) provided in the previous submission of this DID and being updated and revised.

In these scenarios, it is not intended to demonstrate the statistical mean of MDT through a sample size and series of tests, but rather to demonstrate the capability to achieve the MDT during operations. This can be demonstrated in one Failover test for each timed scenario by accomplishing failover or switchover within the required MDT time.

FOS Critical Command and Control Systems are systems that provide critical real-time functions to support the following: launch, early orbit checkout, disposal, orbit adjustment, anomaly investigation, recovery from safe mode, routine real-time commanding and associated monitoring for spacecraft and instrument health and safety. This includes the execution and control of the ground script; the uplink of spacecraft loads, instrument loads and real-time commands; command verification; ingest and monitoring of the real-time housekeeping telemetry and replay telemetry; and the capture and recording of real-time deviations to the planned ground script to ensure that the as-flown ground script is accurate.

For Release B, the FOS Critical Command and Control Systems that perform critical real-time functions consist of redundant groups of Real-Time Servers, Data Servers (for Events archiving function only), User Stations, RAID (Redundant Array of Independent Disks) storage devices, Time Systems, and network equipment (concentrators and hub/bridge assemblies).

#### **4.2.2 Evaluate Fault Detection/Isolation Methods**

The Management Subsystem (MSS) Fault Management Application Service will be implemented in Release B and functions in each of the proposed Science failure scenarios as the primary fault detection capability. Alerts and reports may initiate further fault/failure isolation and subsequent trouble shooting using COTS diagnostic tools as appropriate. All the proposed Science failure scenarios MD 1-4 exercise this fault detection objective and reference the AT and SV test procedures created for Fault Management. The conduct and results of these applicable tests will provide the opportunity to evaluate Fault Management.

#### **4.2.3 Evaluate Ability to Achieve LRU Replacements On-site**

The intent of this objective is to conduct an evaluation of the on-site corrective maintenance capability, consistent with the Release B COTS Maintenance Plan (613-CD-003-001). An analysis of the COTS site corrective maintenance processes to be implemented during Release B, and evaluation of the training and certification processes to achieve and maintain proficiency of assigned personnel, will achieve this objective. Additionally, a review and analysis of the COTS hardware corrective maintenance actions in the EDF and DAACs over the last several years will provide assessment of the COTS maintenance vendor and third party maintenance processes in effect. It is recognized that the vendor response times effective for the EDF are not as stringent as will be required for on-site operations. No MD failure scenario specific to these corrective maintenance process evaluations has been created, but this analysis will be included in DID 519.

Release B COTS will be under vendor maintenance contract during the AT period, and a COTS HW failure after detection, isolation, and confirmation of hardware failure will be corrected on-site by the maintenance vendor. This unplanned, unrehearsed failure activity will also provide a demonstration and assessment of this maintenance approach. The fault detection activities, operator response, local maintenance coordinator diagnosis and fault isolation process, COTS vendor contact and support, LRU identification and changeout, vendor spares positioning and availability, corrective action verification, and maintenance data collection can all be observed and analyzed as unplanned and unrehearsed actions. This unscheduled opportunity provides a demonstration of real failure corrective action processes.

This page intentionally left blank.

# Appendix A Failure Scenarios

---

## A.1 Evaluate Management SubSystem (MSS) Fault Management Application Service

Test No.: MD - 1 Release B

AT/SV Test Cases: B080140-010 Emergency and Other Abnormal Shutdown and Recovery from Catastrophic Emergency Shutdown

B080620-010 Fault Detection, Isolation, and Analysis

B120110-050 End-to-End Fault Management

Fault Management System Verification test procedures

**Test Title:** Evaluate Management SubSystem (MSS) Fault Management Application Service

### Failure Scenario Description:

This scenario is designed to evaluate the capability, effectiveness, and useability of the Fault Management Service to detect, document, diagnose, isolate, provide impact status, and facilitate recovery from faults. The evaluation will be in the context of normal ECS on-site operations being interrupted by planned hardware fault events or simulations with the focus on the effectiveness of this service in identifying and facilitating the accomplishment of corrective actions at the local site level. Local operator, maintenance coordinator, and system administrator interactions with the service and its responsiveness and useability will be evaluated.

**Input:** Standard ECS site operating environment; manual disconnection of the HW or network to simulate a failure, or introduction of real component failure.

### Output:

Configuration status and fault event message displays/printouts; generated datasets.

### Success Criteria:

Following HW failure, operators receive fault error messages detecting and isolating failure to the specific COTS HW. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. The Fault Management Service facilitates and assists the user, operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. The service facilitates and enhances operator corrective action decision processes with accurate and useful operational status and diagnostic tools allowing the operator to determine recovery alternatives, if available, and failure impacts to operations processes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

## **A.2 MSS Critical Services Failure Recovery**

**Test No.:** MD - 2 Release B

**AT Test Case :** TBD

**Test Title:** MSS Critical Services Failure Recovery

### **Failure Scenario Description:**

This scenario evaluates the failover design of the server providing the MSS Critical Services in meeting the MSS function RMA MDT requirement of 20 minutes or less. A fault event in the server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure and local operator/administrator action will be taken to confirm the failure and identify the appropriate recovery corrective action. When switchover is part of the appropriate recovery corrective action, the switchover to the Failover server and resumption of Critical MSS Services should be completed within 20 minutes.

**Input:** Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

### **Output:**

Configuration status and fault event message displays/printouts; generated datasets.

### **Success Criteria:**

Following HW failure, operators receive Fault error messages detecting and isolating failure to the specific MSS Server. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in identifying the appropriate recovery corrective action required. When switchover is part of the appropriate recovery corrective action, the switchover to the Failover MSS Server and resumption of Critical MSS Services will be completed within 20 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

### **A.3 Primary Science Data Receipt Capability Failure Recovery**

**Test No.:** MD - 3 Release B

**AT Test Case :** TBD

**Test Title:** Primary Science Data Receipt Capability Failure Recovery

#### **Failure Scenario Description:**

This scenario evaluates the failover design of the Ingest server providing the primary science data receipt capability to meet the RMA function switchover time requirement of 15 minutes or less. A fault event in the Ingest server is simulated or a planned component failure is introduced to create the failure. The Fault Management Application Service will detect the failure and local operator/administrator action will be taken to confirm the failure and identify the appropriate recovery corrective action. When switchover is part of the appropriate recovery corrective action, the switchover to the failover server and resumption of science data receipt capability should be completed within 15 minutes.

**Input:** Standard ECS site operating environment; MD test plan for the specific HW failure; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

#### **Output:**

Configuration status and fault event message displays/printouts; generated datasets.

#### **Success Criteria:**

Following HW failure, operators receive Fault error messages detecting and isolating failure to the specific Ingest Server. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in identifying the appropriate recovery corrective action required. When switchover is part of the appropriate recovery corrective action, the switchover to the Failover Ingest Server and resumption of science data receipt capability will be completed within 15 minutes. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

## **A.4 Network Failure Recovery**

**Test No.:** MD - 4 Release B

**AT/SV Test Cases:** B080140-010 Emergency and Other Abnormal Shutdown and Recovery from Catastrophic Emergency Shutdown

B080620-010 Fault Detection, Isolation, and Analysis

B120110-050 End-to-End Fault Management

**Fault Management System Verification test procedures**

**Test Title:** Network Failure Recovery

### **Failure Scenario Description:**

This scenario evaluates the ability to detect, diagnose, analyze, and report network faults and errors, at both the local site and SMC levels, and also the local maintenance coordinator's responsiveness in taking appropriate corrective action. A network failure is simulated or a real component failure is introduced in a network hardware device. The fault management capability will detect the failure and facilitate isolation to the device and the diagnosis of the problem. Appropriate alerts will be generated. If the COTS network hardware device is designed with hot swappable components, the failure will evaluate the local site's effectiveness in accomplishing the needed hot swap using available component LRUs. The hot swap can either be simulated or accomplished. The network will be maintained in normal operational status.

**Input:** Standard ECS site operating environment; manual disconnection of the HW to simulate a failure, or introduction of real component failure.

### **Output:**

Configuration status and fault event message displays/printouts; generated datasets.

### **Success Criteria:**

Following network device failure, operators receive fault error messages detecting and isolating failure to the specific device. The network has remained operational with no data loss. Appropriate diagnostics can be executed to further diagnose the specific hardware fault and/or failed LRU. Fault Management facilitates and assists the operator, local maintenance coordinator, or system administrator in specifying and accomplishing the corrective action required. If this test is a real hot swappable component failure, the changeout of the LRU is accomplished using on-site spares, or this can be simulated. Configuration display pages accurately portray the HW configuration before, during, and after the HW failure.

## **A.5 FOS Network Fault Recovery**

**Test No.:** MD - 5 Release B

**FOS AT Test Case:** SYS-2030B - Failure Recovery and Status Monitoring

**Test Title:** FOS Network Fault Recovery

### **Failure Scenario Description:**

This scenario is designed to verify the capability to recover from failures of network components supporting FOS operations, including the Operational LAN (FDDI-Fibre Distributed Data Interface), Ethernet and hub failures, and EOC router failure.

The scenario begins with the sign-on of several user stations and the initialization of the EOC. Configuration and event pages are displayed and used to verify the EOC configuration following logical string assignments and reconfiguration activity performed by the user with ground configuration authority. Logical string assignments supporting real-time, simulation and replay strings are performed for each supported mode (i.e. operational, test, and training). Following string assignments, each type of failure listed above is performed sequentially, with test steps included to ensure the recovery from each failure.

During recovery operations, alphanumeric display pages showing the FOS configuration components and status are viewed and printed at specified times (i.e. before, during, and after failure recovery) in order to verify the accurate representation of configuration information throughout the recovery period.

### **Input:**

Startup scripts for initializing the EOC; manual disassembling/disabling/disconnecting connected network components to simulate network/hub failures or to introduce real component failures.

### **Output:**

Configuration status display pages/printouts and event displays/printouts at EOC/IST-Instrument Support Terminal user stations.

### **Success Criteria:**

Following FDDI and FDDI hub failures, FDDI ring wraps autonomously with no data loss and FOS software applications continue as normal. During Ethernet failure, the EOC user stations on the Ethernet link lose connection to supported logical strings; the affected user station(s) successfully re-establishes former string connection on another EOC user station. Following EOC router failure and recovery, no FOS reconfiguration is required; IST user stations, following ECS Command Language (ECL) directives to reconnect to established logical strings, are successful in connecting. Upon any network failure, connected EOC/IST user stations receive error messages concerning the failure, and messages following network recovery. Configuration display pages accurately portray the FOS configuration before, during and after network failures.

## A.6 FOS Real-Time Server Failure Recovery

**Test No.:** MD - 6 Release B

**FOS AT Test Case:** SYS-2030B - Failure Recovery and Status Monitoring

**Test Title:** FOS Real-Time Server Failure Recovery

### **Failure Scenario Description:**

This scenario is designed to verify the capability to recover from a real-time server failure during real-time operations within a down time of one minute or less.

The scenario begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and the receipt of real-time telemetry. The real-time server is disconnected/powered down to simulate a failure, or a prepared component failure is introduced. Upon detecting telemetry data dropout and other event messages at connected EOC and IST user stations, the ground controller enters directives to transfer control to the backup, specifies the real-time server that is to receive control, and specifies if checkpoint information (telemetry and command path information) is to be applied. As the backup logical string is converted to active, the ground controller requests command authority, resumes the ground script and begins processing real-time telemetry.

### **Input:**

Startup scripts for initializing the EOC; manual disassembling/disabling/disconnecting real-time server to simulate server failure, or introduce real component failure.

### **Output:**

Configuration status and event message displays/printouts.

### **Success Criteria:**

Following server failure, EOC/ISTs receive event messages stating real-time data dropout, pause of the ground schedule, and server failure events. Request of ground configuration authority is granted following failure of the server. Directives to transfer control to the backup real-time server, and transfer checkpoint information are successful **and occur within one minute of request**. Previously running ground script resumes upon ECL directives. EOC/IST users connected to the failed real-time server are re-established to previous logical strings upon re-issue of connection directives. Configuration display pages accurately portray the FOS configuration before, during and after the real-time server failure.

## **A.7 FOS Data Server Failure and Recovery**

**Test No.:** MD - 7 Release B

**FOS AT Test Case:** SYS-2030B - Failure Recovery and Status Monitoring

**Test Title:** FOS Data Server Failure Recovery

### **Failure Scenario Description:**

This scenario is designed to verify the capability to recover from a data server failure during real-time operations.

The scenario begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings. Several analysis requests for datasets are generated and submitted. During execution of the datasets, the data server is disconnected/ powered down to simulate a failure, or a prepared component failure is introduced. Upon detecting event messages stating communications failure with the data server appropriate corrective actions are taken. Configuration display pages are printed before, during and after failure recovery to ensure accurate portrayal of the FOS equipment configuration.

### **Input:**

Startup scripts for initializing the EOC; manual disconnection of the data server to simulate a failure, or introduction of real component failure.

### **Output:**

Configuration status and event message displays/printouts; generated datasets.

### **Success Criteria:**

Following server failure, EOC/ISTs receive error messages stating communications failure of the data server. Initialization and startup of the non-active data server completes within five (5) minutes. Configuration display pages accurately portray the FOS configuration before, during and after the data server failure.

## **A.8 FOS User Station Failure Recovery**

**Test No.:** MD - 8 Release B

**FOS AT Test Case:** SYS-2030B - Failure Recovery and Status Monitoring

**Test Title:** FOS User Station Failure Recovery

### **Failure Scenario Description:**

This scenario is designed to verify the capability to recover from a user station failure during real-time operations within a down time of one minute or less.

The scenario begins with the sign-on of several user stations and the initialization of the EOC, including establishment of logical and backup strings, execution of the ground script, and the receipt of real-time telemetry. The EOC user station currently operating as the ground controller/command issuer is disconnected/powered down to simulate a failure, or a real prepared component failure is introduced. Upon detecting the failure, the ground controller transfers to another EOC user station, requests command authority, applies checkpoint information to the ground script and resumes the script. Steps are also provided to ensure failure recovery from an IST user station failure.

### **Input:**

Startup scripts for initializing the EOC; manually disconnecting the user station to simulate a failure or introduction of component failure.

### **Output:**

Configuration status and event message displays/printouts.

### **Success Criteria:**

Request of ground configuration authority, transfer of checkpoint files to the ground script, and resumption of the ground script is successful **within a down time of one minute or less**, following the issuance of the directives from another EOC user station. Configuration display pages accurately portray the FOS equipment configuration before, during and after the user station failure. IST users experiencing failure conditions may sign on to another IST user station, and perform functions mirroring their previous activity on the failed user station.

## **Appendix B FOS Failure Recovery and Status Monitoring Test Plan**

---

Original version being revised.

This page intentionally left blank.

## Appendix C Science Ingest Failover Test Plan

---

Under development.

This page intentionally left blank.

# Appendix D MSS Critical Services Failover Test Plan

---

Under development.

This page intentionally left blank.

# Abbreviations and Acronyms

---

A <sub>o</sub>	Operational Availability
ASF	University of Alaska Synthetic Aperture Radar (SAR) Facility
AT	Acceptance Test
CCB	Configuration Control Board
CDR	Critical Design Review
CDRD	Contract Data Requirement Document
CDRL	Contract Data Requirements List
CM	Configuration Management
COTS	Commercial Off-the-Shelf
CSMS	Communications and Systems Management Segment
CSS	Communications subsystem
DAACs	Distributed Active Archive Centers
DCN	Document Change Notice
DID	Data Item Description
EBNet	EOSDIS Backbone Network
ECL	ECS Command Language
ECS	EOSDIS Core System
EDC	Earth Resources Observation Systems (EROS) Data Center
EDF	ECS Development Facility
EOC	EOS Operations Center
EOS	Earth Observing System
EOSDIS	Earth Observing System (EOS) Data and Information System (DIS)
EROS	Earth Resources Observation Systems
ESD	Electrostatic Discharge
ESDIS	Earth Science Data and Information System
ESN	EOSDIS Science Network
FDDI	Fiber-optic Distributed Data Interface
FMEA	Failure Modes, and Effects Analyses
FOS	Flight Operations Segment
GSFC	Goddard Space Flight Center

HW	Hardware
IATO	Independent Acceptance Test Organization
ILS	Integrated Logistics Support
IMS	Information Management System
ISS	Internetworking Subsystem
IST	Instrument Support Terminal
JPL	Jet Propulsion Laboratory
LaRC	Langley Research Center
LMC	Local Maintenance Coordinator
LRU	Line Replaceable Unit
M&O	Maintenance and Operations
MD	Maintainability Demonstration
MDT	Mean Down Time
MSS	Management Subsystem
MTTR	Mean Time To Repair
NA	Network Administrator
NASA	National Aeronautics and Space Administration
NSIDC	University of Colorado, National Snow and Ice Data Center
OEM	Original Equipment Manufacturer
OPPM	Outside PPM Hours
ORNL	Oak Ridge National Laboratory
PAIP	Performance Assurance Implementation Plan
PAR	Performance Assurance Requirements
PM	Preventive Maintenance
PPM	Principal Period of Maintenance
RAID	Redundant Array of Independent Disks
RMA	Reliability, Maintainability, and Availability
SA	System Administrator
SDPS	Science Data Processing Segment
SMC	System Monitoring and Coordination Center
SOW	Statement of Work
SV	System Verification
SW	Software
TOO	Target Of Opportunity